2008-06-00

Paramilitary Terrorism A Neglected Threat

Tallen, Bill

Monterey, California. Naval Postgraduate School

Homeland Security Affairs (June 2008), v.4 no. 2
http://hdl.handle.net/10945/24972

Paramilitary Terrorism: A Neglected Threat

Bill Tallen

At 0830 on an otherwise normal autumn morning, a wave of violence erupts without warning at locations across the American heartland, targeting schools and schoolchildren. Improvised explosives detonate in sidewalk trash bins; school buses are bombed; lone snipers target campuses and first responders in hit and run attacks. As confusion and panic spread from local venues to the national consciousness via the twenty-four-hour news media, a band of armed terrorists take over an elementary school in a small Midwestern city. City and county SWAT officers respond to the scene before the scope of the event is clear; trained to respond to a Columbine-like active-shooter incident, they stage a hasty assault which is bloodily repulsed.

Executing a score of adult hostages as evidence of their resolve, the terrorists then herd hundreds of schoolchildren and staff into the school gymnasium, which they prepare with explosives. They upload images of their action onto the Internet. Their postings identify the perpetrators as al Qa'ida-affiliated jihadists. Intelligence from the police perimeter indicates thirty or more fighters, with military small arms, explosives, and heavy weapons, rapidly improving their defenses.

The terrorists announce their intention to execute their hostages, and their willingness to accept 'martyrdom,' in the event of another assault or if the U.S. government does not take immediate steps to meet their single, non-negotiable demand: withdrawal of all American forces from Iraq, Afghanistan, Saudi Arabia, and the rest of the House of Islam.

The scenario above is loosely based on the seizure of Beslan School #1 in the Russian republic of North Ossetia in 2004, where over a thousand hostages were taken, and hundreds of schoolchildren and other innocents were ultimately killed by Chechen terrorists.[1] This attack was conducted by terrorists using conventional weapons and tactics, and required technical expertise less challenging and far more common than the piloting skills that guided commercial jets into American buildings on September 11, 2001.

The Beslan siege lasted three days before ending in massive bloodshed during an assault by government forces – very unlike the instantaneous effects and protracted aftermath that characterize suicide terrorism. The attackers took physical control of high value assets (for what assets are more valuable, in both real and symbolic terms, than our children?), exploited their act for propaganda value, assaulted and murdered hostages throughout the siege, and threatened yet worse consequences if their impossible demands were not met by the Russian government. Although we can only speculate regarding their ultimate intent, which was pre-empted by the government forces' emergency assault, the final outcome in Beslan was terrible enough.

Related scenarios in a U.S. setting are not difficult to construct, applying similar means of attack against a range of soft targets of great iconic, political, or economic value. Attacks on better-protected targets such as nuclear power plants, nuclear materials shipments, or seats of government are generally considered less likely, although surveillance and reconnaissance are known to occur, and some of these harder

targets may actually be more vulnerable to seizure and exploitation by paramilitary forces than they are to suicide terrorism.

From the standpoint of preparedness and response planning, such scenarios bear little resemblance to the Weapon of Mass Destruction (WMD) scenarios that command so much of our national attention. Assaults by armed groups, employing improvised explosive devices (IED) as enablers or force multipliers rather than the primary mechanisms of attack, are commonplace tactics of terrorists and insurgents worldwide. By contrast, effective WMD attacks, no matter how theoretically attractive to terrorists, and how extreme their potential consequences, remain so far the stuff of fiction. While paramilitary attacks may not offer first-order effects (casualties and physical damage) equivalent to those of large-scale WMD, their psychological and strategic impact – and thus their appeal as quintessential acts of terror – may be enormous.[2]

WMD terrorism against U.S. targets may be less likely than more conventional forms of attack. Preparedness and defense against terrorism is a risk-management exercise, and the calculus of likelihood versus consequence – of most dangerous versus most likely – will be ignored at our great peril. The threat of WMD terrorism has led logically to a heavy emphasis on prevention by the intelligence and law enforcement communities. But in the event that prevention fails, WMD terrorism scenarios leave little scope for intervention, as the execution phase would likely be brief and spectacular. For this reason, policy efforts and the allocation of resources have focused heavily upon consequence management and forensics. This tendency is further reinforced by America's recent experience of natural and man-made catastrophes (e.g. Hurricane Katrina and the California fires of 2007), and the structures and processes of consequence management address both terror and non-terror scenarios. The fixation of official attention and resources upon WMD terrorism, and upon consequence management more generally, has left America ill-prepared to respond quickly and effectively to a terrorist paramilitary attack, which may be far more likely than an apocalyptic WMD scenario. Measures should be taken to narrow this gap in preparedness before it can be exploited by our intelligent, opportunistic enemies.

LIKE A DEER IN THE HEADLIGHTS

Although there is informed debate over the attractiveness of WMD to al Qa'ida and its jihadist affiliates, the specter of WMD attack has led U.S. homeland security policy, planning, organization, and operations to concentrate overwhelmingly on either preventing or mitigating the consequences of such attacks.[3] The technical, law enforcement, and intelligence challenges of prevention, and the massive costs and organizational requirements of consequence management, have dominated the attention, efforts, and assets of the interagency community charged with homeland security. The national trauma of Hurricane Katrina in 2005 diverted official attention from terrorism as a causative agent, but reinforced the fixation on consequence management. Agencies charged with response to domestic terrorism are largely the same that have been mandated, since Katrina, to better prepare for the aftermath of future natural disasters.

Since the September 11, 2001 terrorist attacks brought a sense of urgency to U.S. counterterrorist (CT) planning, a large body of official policy and doctrine has emerged. While successive generations of guidance show increasing sophistication in many areas, they are quite consistent in ignoring modalities of terrorist attack other than WMD,

isolated IEDs, and suicide terrorism. The two latter categories receive minimal attention, and in any case they share a salient characteristic of WMD attacks: we either prevent them or clean up and investigate in the aftermath. A selective review of the literature provides illustrative examples.

Homeland Security Presidential Directive-5 (HSPD-5) in 2003 provided course corrections and guidance for most subsequent efforts in the field of federal emergency preparedness. It called for a National Incident Management System (NIMS) to guide the response to domestic incidents "regardless of cause, size, or complexity."[4] It required the development of a national response plan to "integrate Federal Government domestic prevention, preparedness, response, and recovery plans into one all-discipline, all-hazards plan."[5] Significantly, it directed that crisis management and consequence management, previously treated as separate yet related functions, be approached henceforth as an integrated whole.[6] Conflating terrorist attacks with natural or other manmade disasters, and failing to differentiate response to an ongoing incident from mitigation of its after-effects, HSPD-5 set the tone for future policy and planning.

The *National Response Plan* (NRP) was first promulgated in 2004, was later revised to address shortfalls identified in the Hurricane Katrina response, and is now being supplanted by the *National Response Framework* (NRF).[7] Both documents consistently profile the terrorist threat as a nexus of suicide terrorism and WMD – 9/11 writ large – reflecting an already pervasive, and entirely logical, emphasis on prevention as the first line of defense. They pay scant attention to resolving an ongoing crisis of a non-WMD nature, in the event that prevention fails. Both the NRP and NRF are devoted primarily to consequence management, either of WMD attacks or natural disasters.

The lack of attention paid to resolution of an ongoing terrorist incident is also evident in the *National Planning Scenarios*, designed to provide focus for exercises and contingency planning by all levels of government.[8] These fifteen scenarios include two natural disasters, an outbreak of pandemic influenza, and twelve terrorist attacks: one improvised nuclear detonation, one radiological dispersion device, four biological and four chemical attacks, one cyber, one radiological, and one attack using multiple conventional explosives. In several scenarios, terrorists conduct multiple simultaneous or closely sequenced attacks, at varying distances from one another. Effects, especially in the biological and radiological attack scenarios, are spread over time depending on levels of transmissibility or exposure, but attack execution is essentially instantaneous, and the scope of government response is limited to consequence management and criminal investigation in the aftermath.[9] Nowhere in the *National Planning Scenarios* is there a requirement for a tactical response to resolve an ongoing situation or disrupt terrorist actions in progress.

With only rare exceptions, other DOD and Department of Homeland Security (DHS) guidance describe a terrorist threat based primarily on mass-casualty WMD attacks.[10] While the threat of terrorist use of IEDs on a less apocalyptic scale is gaining traction in recent guidance, attention is still directed overwhelmingly to either prevention or post-attack measures.[11]

Nothing in this argument is meant to denigrate the importance of criminal investigation in the aftermath of an attack, nor of the substantial and thus far successful efforts of the intelligence and law enforcement communities to prevent major acts of domestic terrorism. While these are important and worthy efforts, a fixation upon WMD terrorism has combined with the recurring national experience of other manmade or

natural disasters to focus planning efforts and resources to a dangerous degree on the challenges of prevention, investigation, and consequence management. When deterrence, detection, and prevention fail, we will face enemies that must be engaged and defeated – missions with a very different set of requirements.

COMMAND AND CONTROL

Unity of command and clearly defined command and support relationships, across a wide spectrum of responding agencies, would be essential in the event of a time-sensitive and ongoing terrorist incident. The NRF and other national response guidance offer an architecture for command and control (C2) that could well prove cumbersome, confusing, and unresponsive in such a crisis, however sensitive it may be to political and statutory relationships, and however workable under the less constrained timelines of disaster response or consequence management.

A terrorist incident beyond the response capabilities of local and state government – which a Beslan-like attack would certainly be – would trigger requests for federal assistance and invoke federal guidance identifying the Department of Justice, and more specifically the FBI, as lead federal agency. The water is muddied somewhat by the designation of the Department of Homeland Security as lead agency for coordination of incident response generally, across all levels of government.[12] It is made no clearer by DOD's status as lead agency for homeland defense: the seam separating homeland defense from homeland security is not well defined, particularly in the context of an ongoing attack by foreign-based terrorists.[13]

Planning guidance identifies these seams and ambiguities as strengths, which they might well be, if national decision makers have the time and situational awareness to capitalize on the flexibility and adaptability of a vaguely defined system, tailoring it to the exigencies of the moment.[14] In the critical early stages of a terrorist incident this ambiguity may instead challenge the nation's ability to produce a coordinated, effective response.

Critical real-time intelligence, requests and authorizations for assistance, deployment orders, and assignment of command responsibility must flow through the "wiring diagrams" of NIMS among local agencies and three federal departments (DHS, DOJ, and DOD) with overlapping responsibilities, and then to their component agencies, services, and commands. It may be a gross understatement to suggest that this may not occur smoothly in the early hours of a crisis.

A Request for Assistance (RFA) by military forces, for instance, can originate from a state governor's office, or from a federal agency on scene. It will travel through federal law enforcement channels to the attorney general, from there to the Office of the Secretary of Defense for approval, and then to U.S. Northern Command (USNORTHCOM), which only then receives operational control of active duty forces from other combatant commands.[15] If the forces allocated for response include National Guard – which would likely be mobilizing simultaneously under state authority – further coordination of their status and chain of command will be necessary. There are ample opportunities in this process for confusion and delay, which could have particularly (and literally) fatal consequences in an ongoing terrorist incident of the type anticipated here.[16]

NIMS and the Incident Command System promote the concept of Unified Command, a tool for consensus decision-making that can help defuse conflict and integrate civilian

agencies with overlapping responsibilities and jurisdictions.[17] Military forces, however, do not operate under the Unified Command structure at all, and each civilian agency, while participating, maintains a separate chain of command for its own forces, so Unified Command at best provides only unity of effort.

Under the conditions of ambiguity, overlapping responsibilities, compressed timelines, and cascading consequences that will prevail in the event of an ongoing terrorist attack, mission success will require high levels of coordination, shared assumptions, and good will among a multitude of agencies unaccustomed to cooperation in a crisis. Higher echelons and tactical responders alike will require true unity of command, but there is no construct in NIMS that will enable it.

The NIMS command structure has proven useful, or at least usable, in the consequence management scenarios for which it was primarily designed. When rapid, forceful, coordinated tactical response is required to resolve an ongoing terrorist action, convoluted routing of requests for assistance, parallel chains of command, and the consensus decision making of Unified Command will likely fall short of the need.

TIME, SPACE, AND FORCE

One lesson starkly evident in the aftermath of Beslan is that tactical response to such an incident requires discipline, proficiency, and precision. To deny an adversary time to consolidate his position, cause further damage or loss of life, or exploit the propaganda value of his action, the response must also be swift – measured in hours, not days. Rapid deployment of tactical forces capable of resolving the situation is therefore vital.[18]

Local law enforcement agencies (LLEA) would respond quickly, but in most cases lack the ability to defeat numerous, well-prepared adversaries like those that attacked Beslan in 2004.[19] Hostage rescue or asset recovery on the scale envisioned by this scenario is beyond the capability of most LLEA SWAT (Special Weapons and Tactics) teams.[20] Most local and state agencies field teams composed of patrol officers, who receive additional specialized training and equipment, but train and operate as a team only on an occasional basis, and require time to assemble and orient to a crisis situation. These teams seldom consist of more than a dozen assaulters, with varying degrees of support by snipers, breachers, and other specialists.[21] Some departments do field full-time, well-equipped and highly proficient SWAT teams that can respond quickly and in strength to local incidents with a high level of cohesion and tactical proficiency. But even these teams would be challenged by the paradigm shift involved in confronting paramilitary terrorism. Whether full-time or part-time, LLEA SWAT teams quite understandably tend to focus their resources and training time on the scenarios they most frequently confront, such as high risk warrant service, active shooters, and barricaded suspects.

Tactics, techniques, and procedures (TTP), and rules for the use of force which are suitable, legal, and constitutionally defensible for these situations, are often dangerously incompatible with the requirements of combat against multiple, dedicated, heavily armed and fortified terrorists.[22] For instance, the 1999 Columbine school shootings showed the inadequacy of the common SWAT practice of containment, intelligence gathering, negotiation, and deliberate assault planning when faced with an active shooter scenario. Training for such incidents now often stresses the necessity for rapid intervention by small elements at the earliest possible moment. While this may be a realistic and necessary response to a rampage by one or two criminal sociopaths, it

would fail catastrophically, and could easily provoke a hugely disproportionate response, if the attackers were an organized paramilitary group. The Beslan-like paramilitary terrorism scenario is most emphatically not a typical SWAT incident, and will not be resolved by the methods and resources available to local law enforcement.

The FBI represents the next echelon of response, but it is unlikely that the Bureau could quickly field a tactical capability commensurate with its authority. Its field offices in fifty-six U.S. cities can mobilize SWAT teams composed of special agents who volunteer for this ancillary duty and receive appropriate specialized training. Team size varies, and at the larger field offices may include as many as twenty agents, organized into sniper teams, breachers, and assaulters. As with most LLEA teams, however, FBI SWAT team personnel have other primary duties and are seldom afforded the opportunity to train together as a tactical team more than a few days a month. A larger regional SWAT team can be assembled from these field office elements, but assembly alone could require days, and a composite regional team is even less likely to be capable of fully-integrated tactical operations without yet more time for training and rehearsal. Although they have proven adequate for most of the federal law enforcement contingencies for which they were created, FBI SWAT teams may offer only a limited enhancement of local capabilities in time-sensitive terrorism scenarios.[23]

The FBI's Hostage Rescue Team (HRT), the tactical component of its Critical Incident Response Group, is a large, full-time tactical team – a highly capable, Tier One national asset – but its ability to respond effectively to paramilitary terrorism is subject to the tyrannies of time, space, and force. Without specific prior warning of an imminent attack, it would not be deployed forward from its base in Virginia. It could therefore require many hours of air and surface travel to be mission ready at an incident site, particularly one in the central or western United States, even after the processing of a request for assistance and HRT receipt of alert and deployment orders. The HRT lacks sufficient strength and redundancy in both operators and in its command, planning, support, and transportation capabilities, to respond to multiple attacks or diversions in dispersed locations, a requirement it might well face in the event of a well-planned terrorist attack.[24]

Other federal agencies possess tactical teams with varying degrees of proficiency and availability, but these are mostly relatively small, part-time, ad hoc units like the FBI SWAT teams. They are neither trained nor held in readiness for quick response or for missions outside their agencies' normal jurisdictions and operational profiles. Designated military Quick Response Forces (QRF), as well as the tactical teams of installation security forces, can provide support to civil authorities, given either completion of the RFA process described earlier, or a local commander's determination that immediate response on his own authority is necessary. Few of these forces, however, are properly trained or equipped for counterterrorist operations, and they would introduce additional interoperability and chain-of-command issues to offset any incremental advantage they offer, beyond assistance in perimeter control and other supporting roles.

A few DOD special operations forces (SOF) possess robust counterterrorist capabilities, but their ability to respond effectively to domestic incidents of paramilitary terrorism would be constrained by deployment time, distance, and force size in much the same way as the HRT. The demands of wartime operations overseas further limit the availability and readiness of these military assets. Forces tasked with domestic civil

support in terrorism contingencies are unlikely to be fully dedicated to training and preparation for that mission, carrying it instead as an ancillary responsibility during periods of reconstitution, while rotated stateside out of combat zone deployments.

The Posse Comitatus Act or PCA (Title 18, U.S. Code, Section 1385) limits direct involvement of most Title 10 (active duty) military forces in domestic law enforcement.[25] The extent to which it restricts the utility of military assets in domestic CT roles is by no means resolved. As noted earlier, the seam between homeland security – where civilian agencies lead and counterterrorism is seen as a law enforcement function – and homeland defense missions – where DOD leads and possesses considerable freedom of action – is imprecise and largely untested by real world applications. Some DOD guidance claims that statutory exceptions to PCA, or direct presidential authorization, will result in minimal restriction on its forces' freedom to assist law enforcement even during civil support missions. Other guidance is less sanguine, and the boundaries and authorities are not portrayed consistently.[26]

Academic studies, as well as common perceptions among civil authorities and even within the DOD community, reflect the same ambivalence displayed in DOD guidance.[27] Readiness of local authorities or lead federal agencies to request DOD tactical assets, to integrate them rapidly and effectively, and to entrust them with local command of tactical operations would require a remarkable and apparently not universal degree of confidence in the legal basis for their participation. It would also require a willingness to renounce jurisdictional authority and organizational rivalry and distrust.

Military CT teams in a domestic role would find themselves in an operating environment very unlike those that pertain to most overseas war-fighting missions. While their training and operational methods would in many respects be better suited to the requirements of the situation than those of domestic law enforcement agencies, legal and constitutional restraints will intrude. They would be called upon to work in close cooperation, on compressed timelines, with civilian agencies that do not share their doctrine, equipment, TTP, or C2 structure and methods.

Conflicts over jurisdiction, responsibility, and capacity among responding local agencies, the FBI, and military assets are a form of friction that must be expected – particularly in the absence of frequent joint and interagency tactical response exercises involving critical stakeholders. These stakeholders include LLEA nationwide – not just in a few high-profile "showcase" locations – as well as all FBI field offices, the National Guard of every state, and the full range of Title 10 (active duty military) forces discussed earlier.[28]

In summary, tactical teams that could respond effectively to a terrorist paramilitary threat within the United States are limited in number, size, interoperability, and the speed with which they could respond to many potential incident sites. They would be hard-pressed to respond to multiple simultaneous or closely sequenced contingencies – a limitation that could be exploited by an adversary's use of diversions or secondary efforts. Their ability to coordinate their actions with supporting agencies in a hostage rescue or asset recovery mission against significant opposition, in a domestic environment, remains largely untested.

RECOMMENDATIONS

The foregoing discussion has identified three gaps in the nation's preparedness to meet a paramilitary terrorist attack on U.S. soil: inattention to the threat in scenarios,

exercises, and guidance that drive training and preparation at all levels of government; limited availability and slow deployment times of capable CT units; and the unwieldiness of the command and control structure which would authorize and coordinate their employment. In the context of an ongoing competition for time, resources, and attention several recommendations are offered.

Great returns could be achieved from a modest investment, by reorienting the considerable efforts of the homeland security community to an approach more inclusive of the full range of terrorist threats. Even without major force structure, funding, or top-down C2 and doctrinal changes (although all of these may ultimately be necessary), the gaps in preparedness may be narrowed considerably. Simply widening the focus of exercises to include paramilitary terrorist attack scenarios would highlight areas requiring policy attention, identify work-arounds, and prepare key decision makers for their roles in this type of situation. Proper critiques of such exercises, and wide, effective dissemination of lessons learned to agencies at all levels from local police to DHS, DOD, and DOJ would be critical, and are the most often neglected part of the training process. After-action reviews must be brutally honest, fully documented, and devoid of blame. Participants must set aside egos, as well as interagency rivalries, and welcome the use of their failures – along with their successes – to educate their counterparts nationwide.

Three more components of a likely solution emerge from the preceding analysis. Implementation will require careful consideration of where the domestic counterterrorist mission should reside, but should be shaped by the following assumptions:

- Dedicated, full-time federal counterterrorist units without routine law enforcement duties or orientation can best provide the key tactical competencies required to resolve an ongoing incident.
- Streamlined command and control, cutting the Gordian Knot of the NRF authorization process, could promise rapid commitment of CT units in a crisis.
- Regional basing could drastically reduce deployment time to all parts of the country, compared to the current reliance on centralized assets located on the coasts, while also promoting area familiarity and interoperability with local, state, and other federal agencies in each region.

A Military Solution

Existing studies of the DOD role in homeland security, much like the official literature, focus primarily on support to civil authorities in natural or manmade disasters, and on WMD terrorism scenarios. Certain of their recommendations could nonetheless contribute to improving counterterrorist capabilities. These include the constitution of standing, regionally-based response units with a primary civil support mission, each based on an Army Brigade Combat Team or a Marine Air Ground Task Force, substantially augmented with specialties such as Military Police, Engineers, and Civil Affairs from both active and reserve components. To address the deficiency in CT capabilities posed by this analysis, they might also include dedicated CT teams drawn from U.S. Special Operations Command (USSOCOM). One study suggests a total of three of these reinforced brigades.[29] Another more ambitiously proposes one for each of the ten Federal Emergency Management Agency (FEMA) regions.[30]

Both studies conceive of these response forces as full-time, federally funded Title 10 forces, assigned to USNORTHCOM. Under the current system, USNORTHCOM only receives operational control over active and reserve component formations during a crisis, in response to a Request for Assistance. While active duty forces assigned permanently to USNORTHCOM could presumably respond more quickly once committed, processing the RFA through civilian interagency channels could still delay their commitment, despite their relative proximity to an incident site and their simplified chain of command.

Issues relating to Title 10 versus state active duty or Title 32 status for National Guard components of the proposed regional response forces are not particularly relevant for their counterterrorist components. Maintenance of proficiency in complex perishable skills and the requirement for swift deployment in a crisis both argue for full-time, Title 10 active duty status for the CT teams. For Title 10 forces, however, the ambiguity discussed earlier concerning legal authority – is the mission homeland defense or support to civilian law enforcement – would still beg resolution.

The advantages in response time gained from regional basing would be somewhat offset by the difficulties of ensuring consistent, high quality training and support for dispersed SOF elements no longer centrally based or assigned to USSOCOM. Regional reproduction of the training facilities and infrastructure of USSOCOM is unlikely, suggesting either reduced opportunities for training or regular travel out of region to training sites. Team size would have to be large enough to maintain a capable, responsive element on call for crisis deployments, while accommodating training and administrative requirements. These would not be small teams.

Reliance on DOD for improved domestic CT capabilities would also require: funding for further expansion of SOF, in order to avoid a negative impact on war fighting capabilities and commitments; fencing these units from diversion to other missions; time to identify and assign cadre, and then to recruit, train, and attain operational capability for new CT teams; and finding or improving appropriate basing facilities with ready access to air and ground transportation covering the assigned region. These requirements would also pertain more broadly to the larger project of standing up brigade-size regional response forces, and could introduce significant delays in implementation.

A Civil Approach

A better solution to this problem may be found in an expansion and redeployment of existing FBI counterterrorist capabilities. The existing HRT offers a model for an expanded, regionally-based federal CT force. Depending on how regional boundaries were drawn, two or three "cloned" teams resembling the HRT in strength and organization would constitute a significant improvement in capabilities and responsiveness, for a relatively modest investment in 200-300 additional special agents (plus administrative and support echelons as required). New teams could be built on cadre recruited from field office SWAT teams and the existing HRT, and augmented as necessary from those sources until additional recruitment and training filled their ranks. If these teams were dedicated to the counterterrorist mission, and not utilized in other law enforcement functions, recruiting would not be limited to experienced special agents but could seek outside talent; and their training, rules of engagement, and TTP

could reflect the dire and unique circumstances of combat against paramilitary terrorists in a domestic operating environment.

Given the FBI's existing authority as lead federal agency for response to domestic terrorism, regional CT teams under its direct control would offer a simplified C2 structure and minimize jurisdictional ambiguity and the frictions attendant to multi-agency operations. They would relieve DOD special operations forces of responsibility for domestic CT missions in all but the gravest circumstances.

Such an expansion of agent end-strength, and the necessary support staff and infrastructure, would require a significant increase in FBI budget, but not a disproportionate one in the context of other ongoing increases in federal law enforcement manning and capability (for instance in the effort to improve border protection). Shifting current efforts or personnel without expanding end-strength, beyond the use of existing technical expertise and tactical leadership for cadre, could only damage the Bureau's ability to conduct other vital tasks. Rather than a diversion of resources from other efforts, this should be undertaken as a necessary increase in the nation's investment in security from terrorist threats.

CONCLUSION

In the gap between prevention (where we stake many of our hopes and count many successes) and consequence management (where we currently devote a preponderance of our resources) lies the risk of a technically unsophisticated paramilitary attack on assets we are not prepared to lose, and which might offer tremendous leverage to a ruthless and dedicated adversary. It may be time to heed our own counsel, as stated in JP 3-07.2, *Antiterrorism*:

> Terrorists choose their targets deliberately based on the weaknesses they observe in our defenses and in our preparations. They can balance the difficulty in successfully executing a particular attack against the magnitude of loss it might cause. They can monitor our media and listen to our policymakers as our Nation discusses how to protect itself - and adjust their plans accordingly. Where we insulate ourselves from one form of attack, they can shift and focus on another exposed vulnerability. We must defend ourselves against a wide range of means and methods of attack.[31]

Political, legal, and budgetary considerations will continue to bound the art of the possible; there can be no perfect or impenetrable defense. Prioritization of threats to homeland security will remain a calculus of probability and consequence; but the threat we neglect may well prove to be the one most appealing to the adversary.

Bill Tallen serves in Albuquerque, New Mexico, as the director of Agent Operations, Western Command, for the Office of Secure Transportation, National Nuclear Security Administration. His career with the NNSA, a semi-autonomous agency within the U.S. Department of Energy, spans eighteen years of service as a federal agent, training specialist, and manager, including duties in the Special Response Force program and in the development of tactical doctrine and response planning. He is a 2007 graduate of the national security and strategic studies master's degree program at the U.S. Naval War College in Newport, Rhode Island. Mr. Tallen can be reached at gtallen@doeal.gov.

[1] John Dunlop, *The 2002 Dubrovka and 2004 Beslan Hostage Crises* (Stuttgart: Ibidem-Verlag, 2006), 17-101; and John Giduck, *Terror at Beslan* (Golden, CO: Archangel Group, 2005), 111-143.

[2] The modern lexicon of terrorism offers no broadly inclusive, commonly accepted terminology for the sort of attack suggested here, a key component of which is a force large enough to provide tactical flexibility, security, and combat power both in the initial action and in resistance to government countermeasures. The author uses "paramilitary terrorism" to describe hostage-taking, asset seizure, siege, or assault when they are undertaken (as they were at Beslan) by sizable group of highly motivated individuals trained, organized, and equipped like an infantry or special operations unit but without the status or accountability of a state-controlled military force.

[3] Reuven Paz, "Global Jihad and WMD: Between Martyrdom and Mass Destruction," in *Current Trends in Islamist Ideology, Volume 2,* ed. Hillel Franklin et.al. (Washington, DC: Hudson Institute, 2005), 74-86, argues that despite discussion among Islamist scholars and declarations by certain al Qa'ida leaders and cadre, WMD are less attractive than more conventional 'martyrdom' operations for both technical and ideological reasons.

[4] *Management of Domestic Incidents, Homeland Security Presidential Directive/HSPD-5* (28 February 2003), http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html/.

[5] Ibid.

[6] It is both reassuring and in another sense troubling to note that despite HSPD-5's guidance, DOD continues to differentiate crisis management from consequence management; see Chairman, U.S. Joint Chiefs of Staff, *Civil Support,* Joint Publication (JP) 3-28 (Washington, DC: CJCS, 14 September 2007), I-9.

[7] Department of Homeland Security, *National Response Plan* (Washington, DC: DHS, December 2004), http://www.dhs.gov/xprepresp/committees/editorial_0566.shtm; DHS, *Notice of Change to the National Response Plan,* Version 5.0 (Washington, DC: DHS, 25 May 2006), http://www.dhs.gov/xlibrary/assets/NRP_Notice_of_Change_5-22-06.pdf; and DHS, *National Response Framework (DRAFT)* (September 2007), http://www.fema.gov/pdf/emergency/nrf/nrf-base.pdf. The replacement of a "plan" with a "framework" reflects a realization that the scope of issues and agencies addressed is too broad to permit detailed planning at the national level. The NRF offers more broadly couched conceptual guidance for planning by lower echelons of government.

[8] U.S. Homeland Security Council, *National Planning Scenarios,* Version 20.1 (DRAFT) (FOUO) (Washington, DC: Homeland Security Council, April 2005), https://www.hsdl.org/?restricted/view=hs03-013007-06.pdf&code=49fd66d98d6e98381a76ccc0c13328c2.

[9] The sole exception is in one of the biological warfare scenarios, in which infected individuals travel through the country over an extended time period in order to spread contagion.

[10] Representative samples of the bias toward WMD scenarios include Department of Homeland Security, *Guidelines for Homeland Security: Prevention and Deterrence* (Washington, DC: DHS, Office for Domestic Preparedness, June 2003); Department of Homeland Security, *Homeland Security Threat Assessment: Executive Summary* (Washington, DC: DHS, August 2007); and U.S. Northern Command, *Defense Support of Civil Authorities,* Concept Plan (CONPLAN) 2501-05 (Peterson Air Force Base, CO: USNORTHCOM, 11 April 2006).

[11] *Combating Terrorist Use of Explosives in the United States, Homeland Security Presidential Directive/HSPD-19* (12 February 2007), http://www.whitehouse.gov/homeland/hspd19; U.S. President, *National Strategy for Homeland Security* (Washington, DC: White House, 2007), 20; and Federal Bureau of Investigation and U.S. Department of Homeland Security, *Background Information on Potential Terrorist Targeting of Public Facilities: Joint Special Assessment* (FOUO) (Washington, DC: Department of Homeland Security, Office of Intelligence and Analysis, 10 March 2006), https://www.hsdl.org/?restricted/view=hs03-012507-08.pdf&code=49fd66d98d6e98381a76ccc0c13328c2.

[12] Department of Homeland Security, *National Response Plan*, 9, and *National Response Framework*, 21-22, reflect the specific guidance of *HSPD-5* regarding the responsibilities of the Attorney General and the Secretary of Homeland Security as heads of their respective agencies.

[13] Department of Defense, *Homeland Defense and Civil Support Joint Operating Concept, Version 1.9 (DRAFT)* (Washington, DC: USNORTHCOM, September, 2006), 5-8. Illustrative of the ambiguity of these definitions is their treatment in CONPLAN 2501-05, *Defense Support of Civil Authorities,* in which Paragraph 1d(1) indicates that enemy forces are not expected to be encountered during defense support of civil authorities (DSCA), and that their presence would trigger CONPLAN 2002-05, *Homeland Defense* (U), but notes that antiterrorism measures can still be applicable during DSCA. Elsewhere (Paragraph 1g(3)) it notes that terrorist acts do not fall under any of the exceptions to legal and policy restrictions on military support to law enforcement, discussed further elsewhere in this paper. Counterterrorism is clearly considered part of the homeland defense task set under certain circumstances—but DOD is unambiguously lead agency for homeland defense in any form. A tour through the guidance raises more questions than it answers.

[14] Department of Defense, *Homeland Security Joint Operating Concept* (Washington, DC: USNORTHCOM, February 2004), 8.

[15] JP 3-28, *Civil Support,* II-3–II-7; and CONPLAN 2501-05, *Defense Support of Civil Authorities,* Annex A.

[16] Military commanders are authorized to respond without prior authorization through the RFA process in time-sensitive situations, although it appears unlikely that specialized counterterrorist forces hundreds of miles from the incident scene would deploy on this basis: JP 3-28, *Civil Support,* II-7.

[17] Federal Emergency Management Agency, *National Incident Management System*, FEMA 501/Draft (Washington, DC: FEMA, August 2007), 47-50.

[18] Assorted Russian Federal Security Service and military units arrived at Beslan throughout the twenty-eight-hour period between the initial takeover and the emergency assault which resulted in hundreds of dead hostages. Armed local militia proved even more resistant to command authority, and less attentive to rules of engagement, than the security forces. Inconsistent attempts to negotiate with the terrorists, and the lack of rest or sustenance, affected terrorist morale and discipline but appear to have had little impact on their capabilities or murderous intent. Hostages were abused and killed throughout the siege. Terrorist preparations to resist assault were continuous from the time of the takeover. There is no indication that the passage of time worked to the advantage of the authorities in any fashion. Dunlop, *Hostage Crises,* 51-82. If the seized assets were instead nuclear, radiological, or other CBRNE materials, they would require recovery at the earliest possible moment to prevent catastrophic exploitation by the terrorists.

[19] Thirty-two terrorist bodies were recovered on the scene, but eyewitness reports and professional critiques suggest that the total terrorist force may have numbered between fifty and 70 – with the balance escaping during the poorly coordinated assault. Dunlop, *Hostage Crises,* 41-42.

[20] "SWAT" is employed for convenience here to describe a variety of designations, e.g. Special Response Team, Special Operations Team, or Emergency Response Team.

[21] Collaborative efforts by teams from different jurisdictions are theoretically possible, but the unfortunate reality is that in the time and resource-constrained world of law enforcement, such actions are seldom trained or exercised. The likelihood of cooperation among local agencies resolving a situation of this magnitude is small, thanks to dissimilar tactics, techniques, and procedures (TTP), incompatible communications, and a general lack of experience in planning and conducting dynamic, multi-agency tactical operations on this scale.

[22] Giduck, *Terror at Beslan,* 289-316, offers a detailed analysis of the inadequacies of routine domestic SWAT practices when confronting a Beslan-like threat. This author's experience as a trainer in the Special Response Force Program of the U.S. Department of Energy confirms the importance of a counterterrorist versus law enforcement focus for responders to such incidents.

[23] Federal Bureau of Investigation, El Paso Division, "SWAT and ERT," http://elpaso.fbi.gov/swatert.htm; Special Agent David J. Raymond in telephone conversation with author, 16 October 2007; and the author's observations based on joint training and interaction with FBI regional SWAT team members 2001-2004.

[24] Federal Bureau of Investigation, "Investigative Programs, Critical Incident Response Group: Tactical Support Branch," http://www.fbi.gov/hq/isd/cirg/tact.htm, further explicated by Special Agent David J. Raymond, telephone conversation with author, 16 October 2007.

[25] U.S. Navy and Marine Corps forces are restricted only by customary DOD policy, not by the letter of the law.

[26] For instance, Department of Defense, *Homeland Defense and Civil Support Joint Operating Concept,* 40, and JP 3-28, *Civil Support,* F-2, assert broad authority for Title 10 forces under various statutory exceptions or direct Presidential authorization; but JP 3-28, I-9 cites "legal restrictions which generally preclude DOD from participating in CrM [crisis management] law enforcement investigations and operations." CONPLAN 2501-05, *Defense Support of Civil Authorities*, Paragraph 1g(3) also provides a narrower interpretation of the circumstances permitting military involvement in law enforcement during civil support operations.

[27] Paul Schott Stevens, *U.S. Armed Forces and Homeland Defense: The Legal Framework,* CSIS Report (Washington, DC: Center for Strategic and International Studies, October 2001), 3 and 22-27, argues for broad Title 10 authority, while a more restrictive view is expressed in Jeffrey D. Brake, *Terrorism and the Military's Role in Domestic Crisis Management: Background and Issues for Congress* Washington DC: Congressional Research Service, 27 January 2003), 11.

[28] Author's observations of Department of Energy Joint Training Exercises 1994-present are illustrative of these frictions. In one case (Exercise Digit Pace II, 1997) conflicting assertions of authority by a DOE tactical commander and State Police Incident Commander on-scene resulted in the passage of several hours before the two first met to begin discussions regarding unified command. On another occasion, an FBI Special Agent in Charge (SAC) arrived at an incident scene and asserted immediate LFA command authority in the midst of ongoing tactical operations despite the absence of Bureau resources, communications capability, or situational awareness. Every such occasion generates valuable lessons learned and should contribute to a steep learning curve for all involved – but are these experiences frequent and inclusive enough, or disseminated widely enough, to have broad utility?

[29] Lynn E. Davis, David E. Mosher, Richard R. Brennan, Michael D. Greenberg, K. Scott McMahon, and Charles W. Yost, *Army Forces for Homeland Security* (Santa Monica: RAND, 2004), suggest integration of these three brigades with the forthcoming DHS regional structure. A counterterrorist team is part of the organization proposed by this study.

[30] William W. Johnson, *Active Component Rapid Response Force; The Answer to the Military's Issues with Efficient and Effective Support During Response to and Recovery from Incidents of National Significance*, Advanced Military Studies Program Monograph (Fort Leavenworth, KS: U.S. Army Command and General Staff College, 2007), envisions ten Regional Response Units, a number difficult to provide in an era of limited forces and heavy overseas commitments. Fencing ten brigades out of the overseas deployment cycle may be impossible for at least the near future. However, the alternative of assigning the civil support mission to units reconstituting from a deployment or preparing for their next one would not meet the need for dedicated forces with focused training and planning for their domestic responsibility. A more modest number of dedicated response units, based upon broader regional boundaries than FEMA's, might be advisable.

[31] Chairman, U.S. Joint Chiefs of Staff, *Antiterrorism*, Joint Publication (JP) 3-07.2 (Washington, DC: CJCS, 14 April 2006), II-08.